

SEALED

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
ICLOUD ACCOUNTS ASSOCIATED WITH
EMAIL ADDRESS
JROD14230@OUTLOOK.COM AND PHONE
NUMBER (304) 619-9633 THAT ARE
STORED AT PREMISES CONTROLLED
BY APPLE, INC.

Case No. 2:23-mj-00126

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Nicole S. Pinardo, being first duly sworn, hereby depose
and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for
a search warrant for information associated with certain accounts
that are stored at premises owned, maintained, controlled, or
operated by Apple Inc. ("Apple"), an electronic communications
service and/or remote computing service provider headquartered at
One Apple Park Way, Cupertino, California. The information to be
searched is described in the following paragraphs and in Attachment
A. This affidavit is made in support of an application for a search
warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and
2703(c)(1)(A) to require Apple to disclose to the government copies
of the information (including the content of communications)
further described in Section I of Attachment B. Upon receipt of
the information described in Section I of Attachment B, government-

authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Detective with the Beckley Police Department, Investigative Division. I have been so employed for approximately five years; however, I possess a combined total of approximately eleven years of experience as a law enforcement officer. I have experience in conducting investigations involving computers and the procedures that are necessary to retrieve, collect, and preserve electronic evidence. Through my training and experience, including on-the-job discussions with other law enforcement agents and cooperating suspects, I am familiar with the operational techniques and organizational structure of child pornography distribution networks and child pornography possessors and their use of computers and other media devices.

3. I am a graduate of the West Virginia State Police Academy and hold an active law enforcement certification in the state of West Virginia. I am also currently deputized through the Department of Homeland Security and the West Virginia State Police as a Task Force Officer (TFO). I have specifically received training in the areas of child pornography and the sexual exploitation and abuse of children. This training includes specialized instruction on how to conduct criminal investigations related to violations of child protection laws pursuant to Title 18 U.S.C. §§ 2251, 2252 and 2252A.

4. As a Detective and TFO, I have investigated state and federal criminal violations related to cybercrime, child exploitation, and child pornography. I have gained experience through training as well as everyday work relating to investigations involving the receipt, possession, access with intent to view, production, importation, advertising, and distribution of child pornography that occur in the District of Southern West Virginia. I have received training in the areas of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have obtained search warrants for child pornography offenses, and I have been the case agent or assisted others in numerous investigations involving the sexual exploitation of children. Moreover, I am a law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§2251 (production of child pornography), 2252A(a)(2) (transport, receipt, or distribution of child pornography) and 2252A(a)(5)(B) (possession of and access with intent to view child pornography), and I am authorized by law to request a search warrant.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2251 (production of child pornography) and 2252A (transport, receipt, distribution, possession, and access with intent to view child pornography), 1512(c)(1) (obstruction of justice), and 1519 (destruction of records) (collectively, the "Subject Offenses have been committed by Jarrod BENNETT. There is also probable cause to search the information described in Attachment A for evidence, contraband, and/or fruits of these crimes further described in Attachment B.

II. JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

III. PROBABLE CAUSE

8. On or about April 18, 2023, SnapChat submitted CyberTip Report #157988246 to NCMEC. The incident type was identified as apparent child pornography, and the incident time was listed as: March 10, 2023, 19:29:24 UTC.

9. SnapChat uploaded one image file in connection with the report, which contained apparent child pornography. SnapChat

reported that the file at issue was uploaded or shared by SnapChat username "thatoneguy26520." An email address of healer72@yahoo.com, and an IP address of 184.14.114.149 was provided by SnapChat for identification purposes. Snapchat viewed the entire contents of the uploaded file that was reported to contain child pornography.

10. On or about April 18, 2023, your Affiant reviewed the image file associated to the CyberTip and found it to contain a prepubescent male taking a photo of himself in the mirror while posing nude. This file was uploaded by SnapChat user "thatoneguy26520" on March 10, 2023.

11. On or about April 18, 2023, a State of West Virginia search warrant was obtained and served to SnapChat for all contact and personal identifying information, additional SnapChat accounts associated with the target account, all devices used and otherwise associated with the target account, all activity logs, all photos and videos uploaded by the account user, all profile information, all records of communications and messages made or received by the user, all check ins or any other location information, future and passed events the user responded to, all IP logs and associated port IDs, all records of the accounts usage of the like and follow features, all records of the accounts usage of the share feature, all information about the SnapChat pages that the account is or was a "fan" of, all records of Snap searches performed by the

account, all information about the users access and use of marketplace, the types of services utilized by the user, all privacy settings and other accounts settings, and all records pertaining to the communications between SnapChat and any person regarding the user or the user's SnapChat account associated with the SnapChat user "thatoneguy26520" between the dates of March 1, 2023 through April 16, 2023.

12. On or around May 24, 2023, your Affiant received a digital download of the requested account information from SnapChat for the username "thatoneguy26520."

13. The information received showed the username of "thatoneguy26520" was created on February 20, 2023, and the account was disabled by Snapchat on March 10, 2023. During the 10-day span of information received, it shows the subject had sent approximately 9 different photos and 8 different videos containing material depicting minors in sexually explicit conduct. The suspect had sent these files approximately 26 times to approximately 10 different people.

14. The photos sent included an image of young boys estimated to be approximately 7 years old standing nude, back-to-back, with erect penises and an image of what appears to be a toddler aged female's vagina being penetrated by an adult male's penis. The videos sent include several videos of prepubescent females masturbating and another video shows two young boys estimated to

be around 8 years old nude. In the video one boy performs oral sex on the other boy.

15. Of note, a video from the "Memories" section of the SnapChat account showed what appeared to be a prepubescent female lying face down on a couch with a blanket covering her. The first video zooms in to focus on the child's buttocks. A second video shows a slender white male wearing only boxers stepping towards the child with his erect penis out. As the male is stepping towards the child, he is stroking his penis.

16. Further investigation revealed that the IP address provided in the Cybertip and Snapchat return resolved to Frontier Communications. The account listed a subscriber as Jarrod BENNETT ("BENNETT") with a service address of 115 Yaweh Ln Mount Nebo, WV 26679. At the time, BENNETT was employed as a deputy sheriff with the Nicholas County Sheriff's Department.

17. On June 5, 2023, a search warrant was obtained to search the Mount Nebo residence belonging to BENNETT. The search warrant was executed the same day. During the execution of the search warrant, several electronic devices were seized. It was also discovered that the couch and surrounding area seen in the "Memories" video described in Paragraph 15 matched that seen in the BENNETT residence. It was later learned that an approximately

10-year-old female was residing with BENNETT at his residence.¹ Additionally, BENNETT's physical appearance is consistent with that of the slender white male depicted in the video described in Paragraph 15, and he is the only adult male residing in the home.

18. One seized electronic device was an Apple iPhone 14 Pro cellphone ("the Phone"), which has been forensically reviewed. The review of the aforementioned device, seized from BENNETT at the time of the search, revealed evidence that the iCloud accounts associated with email address jrod14230@outlook.com and phone number (304) 619-9633 had been accessed on the Phone or were associated with websites or applications accessed on the Phone. The Phone also had evidence showing that it was utilized by BENNETT, including accessing email accounts and the use of text messages. The Phone was password protected.

19. During the search warrant execution BENNETT agreed to a non-custodial, voluntary interview with your Affiant and Homeland Security Special Agent Brian Morris. Your Affiant advised BENNETT of the search warrant regarding the search and seizure of his

¹ This minor female was later forensically interviewed and did not make any disclosures of abuse. However, this is not uncommon if a minor victim is asleep when an image or video is produced, and the minor in the video did not appear to be awake. Moreover, at the time of the forensic interview, the minor female and her mother still lived with BENNETT, a law enforcement officer, at his residence.

electronic devices to include cellphones, computers, and external storage devices. BENNETT stated he understood. BENNETT's cellphone number is (304) 619-9633. BENNETT stated that he resided at 115 Yaweh Ln Mount Nebo, WV with his fiancée Tiffany Blankenship.

20. Information from the Phone was extracted by computer forensic analyst ("CFA") Fred Pickering with Homeland Security. On May 26, 2023, BENNETT received an email on his jrod14230@outlook.com account which was sent from SnapChat. The content of this email stated "your account has been reported. Our automated defense has removed the reported content for violating community guidelines around Child Sexual abuse Materials." In the days following the receipt of this email, CFA Pickering located the following Google searches on the Phone: "how to delete SnapChat account," "what happens if your SnapChat is reported," and "how long will my account be locked on SnapChat." The Phone accessed the website <https://notroop.com/delete-your-snapchat-account>. It was discovered BENNETT had installed an application which is specifically used for file moving and cleaning. On June 2, 2023, three days before the execution of the search warrant at BENNETT's residence, a large number of files were deleted from the Phone.

21. Despite these deletions, CFA Pickering was able to locate several files of child pornography on BENNETT's phone which included videos and images of prepubescent females shown nude with their genitals exposed. CFA Pickering also located several images

on BENNETT's phone which corresponded with the images from the SnapChat return in his current photo library.

22. Apple's iCloud service allows you to share photos and videos across devices, while also giving you an automatic backup should something happen to your iPhone. For these reasons, the iCloud's memory is more permanent than the memory on your iPhone and can serve as a failsafe if something happens to your Apple device. Several items can be saved to iCloud as a device backup such as texts, photos, videos, phone numbers, and downloaded application data. Recovered data from BENNETT's phone shows iCloud backups conducted on May 28, 2023, May 30, 2023, and June 2, 2023. It is believed that these iCloud backups will contain pertinent data that is no longer present on the phone.

23. On or about June 8, 2023, law enforcement sent a preservation letter to Apple.

IV. BACKGROUND CONCERNING APPLE²

24. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating

² The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>; "Manage and use your Apple ID," available at <https://support.apple.com/en-us/HT203993>; "iCloud," available at <http://www.apple.com/icloud/>; "Introduction to iCloud," available

system, and desktop and laptop computers based on the Mac OS operating system.

25. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.
- c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create,

at <https://support.apple.com/kb/PH26502>; "What does iCloud back up?," available at <https://support.apple.com/kb/PH12519>; and "Apple Platform Security," available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

- d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

- e. Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags, which are tracking devices sold by Apple.
- f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.
- g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

26. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can

submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

27. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone number. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and

access the account, and other log files that reflect usage of the account.

28. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "capability query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the "Find My" service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

29. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device

identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

30. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Some of this data is stored on Apple's servers in an encrypted

form but may nonetheless be decrypted by Apple. Records and data associated with third-party apps, including the instant messaging service WhatsApp, may also be stored on iCloud.

31. In my training and experience, evidence of who was using an Apple ID, and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

32. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation.

33. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs,

documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

34. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

35. Other information connected to the use of an Apple ID may lead to the discovery of additional evidence. For example, the apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators or potential victims. In addition, emails, instant messages, Internet activity, documents,

and contact information can lead to the identification of co-conspirators, victims, and instrumentalities of the crimes under investigation.


36. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple services. In my training and experience, such information may constitute evidence of the crimes under investigation including, but not limited to, information that can be used to identify the account's user or users; the use of applications through which child pornography is stored, shared, or obtained; communications with minors for the purpose of producing child pornography or child erotica; communication with other individuals involved in the trafficking of child pornography materials; and efforts to delete or destroy electronic records or data, including from an iCloud account.

V. CONCLUSION

37. Based on the forgoing, I request that the Court issue the proposed search warrant.

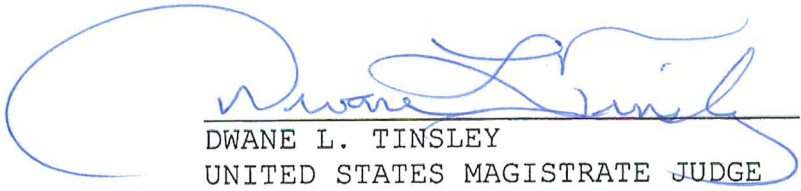
38. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Further your Affiant sayeth naught.



Detective TFO Nicole Pinardo
Beckley Police Department
Department of Homeland Security

Sworn to by the Affiant telephonically in accordance with the procedures of Rule 4.1 this 11th day of July, 2023.



DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF WEST VIRGINIA